REMARKS

Claims 1-79 have been canceled as being drawn to a non-elected invention.

Claims 80 and 81 remain in the application.

Claims 80 and 81 were rejected as being anticipated by U.S. Patent 6,317,834 to Genarro. This rejection is traversed without amendment.

At the outset, it should be understood that the invention embodied in claims 80 and 81 deal with User Identity, that is, who someone claims to be in the context of a computing system. In sharp contrast, Genarro deals with User Authentication, that is, how to ascertain whether a person may rightfully claim the User Identity proferred. Thus, the domain covered by the present invention and the teachings of Genarro are completely different (essentially as different as an ID and a password). Claims 80 and 81 provide an advanced form of ID processing, while Gennaro provides an advanced form of "password" processing (where a Biometric reading is considered part of an extended Authenticator). Conceivably, one might use the two inventions together because they serve completely different functions, but Genarro certainly does not anticipate the claimed invention as it performs a completely different function and uses completely different processing steps.

While it is common practice for an ID and a password (or other authenticator) to occur together, they are quite different entities and serve quite different purposes. There are systems with IDs but no passwords (consider the "public comments" section of many news sites). Likewise, there are systems with passwords but no IDs (consider a door with a combination lock). To demonstrate the well recognized differences between User IDs and authenticators, attached is a printout form the website http://www.oit.nsw.gov.au).

While both the claimed invention and Gennaro use cryptography to preserve privacy, it should be understood that that is one of the standard purposes of cryptography, and any similarity between the claimed invention and Gennaro ends there. The claimed invention provides a mechanism for a plurality of computing systems (e.g., web sites) to cooperate in the service of a user without the sites being able to associate the user's data at one site with that at another (hence the use of a plurality of encrypted identifiers). Specifically, claim 80

requires a first anonymous identifier being determined from the user's personal identifier and being used to access data in a first database; authentication of the user using data in the first database using the first anonymous identifier; and determining a second anonymous identifier from the user's personal identifier and using the second anonymous identifier to access personal information in a second database if the authentication is positive. Figure 9 of the application shows an exemplary embodiment of the invention which may be used in the healthcare industry. Page 40 of the application shows the relationships of a UAI with a W-UAI and PS-UAI, as they relate a password authentication within an exemplary embodiment of the invention; however, as explained on page 40, the methodology of this invention also contemplates use with "digital certificate" where the user is passed to the appropriate Certificate Authority (see lines 10-11 on page 40).

Genarro, by contrast, provides a means for a computing system to hold an irreplaceable authenticator (a biometric) on behalf of the user, without the biometric being vulnerable to theft. Figure 11 of Genarro shows the SAME "Personal Identifier" in Database 1 (186) and Database 2 (184). This is completely opposite of the claimed invention where there is explicitly required a different anonymous identifier for each database.

The claimed invention preserves a user's privacy over a plurality of systems by using cryptography to provide different, but related, identifiers to each system. In a proper implementation of the claimed invention, no two systems can determine that they possess data on the same user, but the authentication can be as strong or as weak as the developer desires (anything from a simple PIN to a sophisticated system such as in Gennarro). In contrast, Gennaro uses cryptography to prevent the theft of an irreplaceable authenticator. In Gennaro, if properly implemented, a number of systems can conclude that they have data on the same user since they share the same "Personal Identifier" (See Figure 11), but an end user would have great difficulty authenticating as anyone other than themselves. Thus, it should be understood that the claimed invention prevents systems from covertly combining their data to get an inappropriately detailed picture of their end users, while Gennaro prevents an end user from inappropriately accessing the data and functions of another user–two very different issues and solutions.

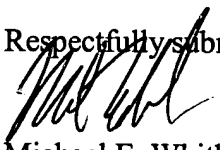
In short, the Examiner's conclusions concerning Gennaro having different first and second anonymous identifiers is simply incorrect (as is demonstrated by Figure 11 of Gennaro) and appears to be a matter of simply confusing identifiers with authenticators as discussed in more detail above. As such, Gennaro wholly lacks several of the features of the claimed invention and does not anticipate the claims.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 80-81 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 50-2041.

Respectfully submitted,



Michael E. Whitham
Reg. No. 32,635

Whitham, Curtis & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190

Tel. (703) 787-9400
Fax. (703) 787-7557

Customer No.: 30743

Home

Welcome to the website of the NSW Government Chief Information Office (GCIO) formerly the Office o Communications Technology (OICT). The website currently references the documents and content of the

Information and Communications Technology (ICT) is a key priority of the NSW Government. The Dep Commerce through the GCIO, plays a leadership role in developing and deploying government wide stra management of ICT within and between government, industry and the community. It is the NSW Govern for ICT issues and electronic services.

The role of GCIO is to use ICT to foster improved value, customer focused services, and improved proce government activity.

Please refer to the Strategies section of this site for further information or Contact Us.

News & Updates

- On-Line Benchmarking Services
- Recordkeeping
- Online Videoconferencing booking system
- Commerce Annual Report

Quick Links

- ROSI Guide
- Enterprise Architecture
- IT Security Bulletin No 3
- Business-Government Task Force on Critical Infrastructure
- Security Survey

What's Popular

- OICT Contacts
- OICT Guidelines
- Virus Alerts and Information
- GovLink
- Human Services BSDP
- *connecting*Business
- Community Technology Centres

Information Security Guideline for NSW Government - Part 3 Information Security Baseline Controls

6. Technical controls

Technical controls must be implemented to ensure confidentiality of data and authorised access to systems is maintained.

Controls must be implemented to restrict access to information, computers, networks, applications, system resources, files and programs.

6.1 Identification and Authentication

Identification is the means by which a user provides a claimed identity to a system. Authentication is the means by which this claim is validated. An identifier or user id is usually a series of non-secret characters that are used to attempt log in to a system. Until the user authenticates himself he will have no access to the system.

The identifier is a mechanism to allow the user access to various resources, files, directories, printers on the system. The identifier must be unique to the user so that he can be held accountable for any actions performed using that identifier. When the user changes his role, is transferred or promoted, then he should have his access rights changed to reflect his new role. When the user leaves the agency, his user identifier should be immediately removed from the system.

Authentication is required before the user can logon to the system. There are three types of "authentication":

- Identification and Authentication based on what a User knows. Passwords and phrases are often used to authenticate users.
- Identification and Authentication based on what a User has. Tokens such as magnetic cards, and smartcards are examples. A common application of magnetic cards is the use of an ATM where the user must possess the card and provide a pin number. Use of a challenge response system such as RSA Secure ID or RACAL Watchword is an example of the use of a smartcard.
- Identification and Authentication based on what a User is. These are biometric measurements or features such as finger prints, retina scans, voice recognition used to authenticate the user.

The security and utility of various authenticators is considered below:

6.1.1 Passwords

Passwords are easy to implement, change and are inexpensive. Most user access systems employ them. Unfortunately they are also the easiest to compromise and require well educated and disciplined users to implement effectively. Bad password management practices contribute to weak password controls.

Examples include:

- Use of simple passwords;
- Writing down of passwords;
- Not changing passwords regularly.

An effective password management policy should include:

- Choosing passwords which are not found in the dictionary;
- Choosing passwords that are a combination of alphabetic characters, numbers and special characters !@#$%^&*() ?;
- Using a combination of upper and lower case characters Ab1E%xcP;
- Choosing passwords with a minimum length of 8 characters;
- Changing passwords every 30 days;
- Not allowing a password that has been used within the last 10 cycles (changes of passwords);
- Unique User ID and passwords for each user to maintain accountability;
- All default User ID's such as Guest should be disabled;
- All User ID's must require a password;
- Not retaining written records of passwords;
- Password confidential must be maintained;
- Passwords not being displayed during entry;
- Requirement to enter old password when changing to new password.

Passwords should be stored in encrypted format using a one way encryption algorithm.

The strength of passwords should be verified by the use of Password cracking programs such as L0phtcrack (available for NT Systems) which can be run by the Systems Administrators. Any weak passwords will be revealed quickly and can then be changed. Other threats to passwords include the use of "sniffers" which eavesdrop on the network and capture password hashes or data for cracking at a later time. Passwords can be compromised simply by viewing what a user types in.

Given the relative weakness of passwords compared to Tokens or Biometrics ICT is strongly recommended that if a system has a high degree of confidentiality attaching to ICT such as payroll, personnel, taxation or medical data, that an authentication method other than passwords be implemented. Token or biometric authentication methods are inherently more secure

6.1.2 Tokens

Tokens provide the capability of having complex one time passwords that the user can never forget. These one time password systems are synchronised with the access system so that only the user possessing the token can gain access. Token passwords usually require the input of a simple PIN known to the user, as well as the one-time password that is displayed on

the token. Use of the PIN provides protection should the token be lost.

Should someone see what the user has entered, when logging into a session, they will not be able to use the password as ICT will be different the next time.

If the user leaves the agency without returning the token then the token can be deactivated.

Tokens provide the one form of authenticator that offers protection from compromise during logon, from a tapped line.

Tokens are usually smartcards, however various versions are now available including a version used with palm tops devices.

The main disadvantage of tokens is that initially they are more expensive than passwords to implement. This cost is continually being reduced. Currently tokens cost approximately $100 each.

6.1.3 Biometric Devices

While these in theory provide the best authentication, they still present problems in practice. Continual improvement will see this technology gain in acceptance, both as the price of readers goes down and as the accuracy and reliability improves. Finger scanning and handwriting devices are examples of biometric devices that are currently available on the market.

Cost and reliability are the main disadvantages at present.

AS/NZS 7799.2:2003
A.9.3.1 User shall be required to follow good security practices in the selection and use of passwords.

AS/NZS 7799.2:2003
A.9.4.3 Access by remote users shall be subject to authentication.

AS/NZS 7799.2:2003
A.9.4.4 Connections to remote computer systems shall be authenticated.

AS/NZS 7799.2:2003
A.9.5.3 All users shall have a unique identifier for their personal and sole use so that activities can be traced to the responsible individual.

AS/NZS 7799.2:2003
A.9.5.4 A password management program shall be in place to provide an effective, interactive facility which ensures quality passwords.